ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT
Departement Maschinenbau & Verfahrenstechnik:
Department of Mechanical & Process Engineering:

Determinism vs. Probabilism, Introduction to Basic Methods and Structure of Probabilistic Risk Assessments (PRA)

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Laboratory for Safety Analysis
INSTITUTE FOR ENERGY TECHNOLOGY

DMAVT
Departement Maschinenbau & Verfahrenstechnik:
Department of Mechanical & Process Engineering:

Scope of Probabilistic Risk Assessment (PRA)

- Both accident initiating events and the unavailability of safety equipment or measures needed to handle accidents are assumed.
- The technical system and specific chains of events (scenarios) including their frequencies of occurrence and resulting plant states are modeled.
- Physical phenomena of the postulated scenarios are modelled, and respective consequences are assessed – inside and outside the plant.
- The risk of the analyzed system is the sum of the products of realistically identified consequences x and their frequencies h(x)
  $R = x1 \cdot h(x1) + x2 \cdot h(x2) + ...$
  for a representative number of exclusive initiating events and event chains.

Deterministic vs. probabilistic approach (1/2)

Deterministic (postulating)

- Events completely determined by cause-effect-chains (causality).
- Analyse of the effects of assumed causes.

Statistically (retrospective)

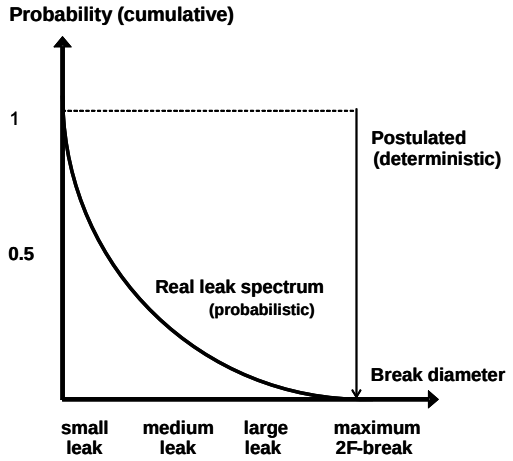
- Rules can be derived from a large number of similar events (based on experience).
- Directly applicable observations can be transferred to the system or to the event level.

Probabilistic (prognostic)

- Events can be identified by the probability of occurrence.
- Use of observations on the level of components (Axiom system of Kolmogoroff).

Deterministic vs. probabilistic approach (2/2)

Example „leakage of the primary coolant boundary"



Approaches		
statistic	**deterministic**	**probabilistic**
a great number of similar events hold experiential values	events are completely predetermined through effect chains (causality)	Events can be identified through their probabilities of occurrence
Methodology (within risk analyses)		
Analyse of a great number of directly usable observations on the level of systems / events	Analyse of the effects of assumed causes on the level of relevant systems / events	Complete analyse of system caused event chains and realistic estimation of frequencies and consequences
(descriptive)	(definitive)	(prognostic)
Risk definition		
risk = expected value ≥ 0		risk = dependent probability
Prerequisites		
relative frequency		Kolmogoroff axiom system

ETH Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich
Laboratory for Safety Analysis INSTITUTE FOR ENERGY TECHNOLOGY
DMAVT Departement Maschinenbau & Verfahrenstechnik Department of Mechanical & Process Engineering

Terms in the Field of Probabilisitc Risk Assessments

- **Events (Examples):**
  - A pump fails within a defined time frame,
  - The wind speed exceeds a certain value within a defined time frame,
  - A great number of events cause physical reactions, etc.
- **Probabilities:**
  - Classical (Laplace): probability as the number of cases in which the event occurs, divided by the number of all possible cases (probability as relative frequency)
  - Frequency related (Mises): probability as a limiting value of the relative frequency of an event after a great (unlimited) number of repetitions under the same conditions.
  - Subjective: probability as a degree of the expectation or the confidence of an individual into a statement that a possible event occurs, a described circumstance occurs, etc.

Defition of some Terms

Absolute Frequency

- How often a given measured value occurs within a sample (≥ 0)

Relative Frequency

- Ratio between the number of certain events to the number of all events (≤ 1)

Probability

- Measure for the uncertainty of future events (between 0 and 1)

Frequency

- Time related frequency (e.g. number per year) (≥ 0)

statistically	probabilistically
Risk = expected value ≥ 0	Risk = related probability
Example: throwing a coin ("heads" = „0" and "tails" = „1")	
$E(X)=\sum_{i=1}^{2} x_i \cdot \hat{\Pr}(X=x_i)$ E(X): Expected value X: Probability variable "heads"/"tails" $\hat{\Pr}(\bullet)$: Relative frequency <u>Observation:</u> $x_i=\begin{cases}1 & \hat{\Pr}(X=x_i)=\frac{550}{1000}=0{,}55\\ 0 & \hat{\Pr}(X=x_i)=\frac{450}{1000}=0{,}45\end{cases}$ $\Rightarrow$ E(X) = 0,55 The „expectation" for „1" is closer to 100%	Risk = Pr(X) = Pr(X|E)·Pr(E) Pr(E): Probability that a coin will be thrown Pr(X): Probability that "1" occurs Pr(X|E): Probability of "1" under the condition that a coin has been thrown Pr(X) = Pr(X|E)·Pr(E) = 0,5·1 = 0,5 The probability of heaving "1" is 0.5 Axiom system of Kolmogoroff: 1. $0 \leq \Pr(x) \leq 1$ 2. Pr(sure event) = 1 3. $\Pr\left(\bigcup_{i=1}^{n} x_i\right)=\Pr\left(\sum_{i=1}^{n} x_i\right)$

Probabilistic Risk Assessments (PRA) in Comparision with Deterministic Approaches

- PRA as a complementary instrument.
- PRA aims at realistic description of risk and safety.
- PRA models provide information on expected performance of different safety measures; they disclose weak points.
- PRA reflects consequences of dependencies and man-machine interdependencies
- PRA shows uncertainties.
- PRA shows the relative importance of each accident sequence, it allows focusing on dominant accident sequences.
- PRA allows optimal allocation of available resources.

Structure and "Levels" of a PRA for Nuclear Power Plants

Plant response to initiating events	→ **Level 1**	Frequency of core damage (CDF) • includes accident management measures
Physical effects, containment response	→ **Level 2**	Frequency and amount of radionuclides released (source term, PDF)
Athmospheric dispersion, potential and expected doses, dose-effect/risk relation	→ **Level 3**	Frequency and quantities of environmental and health effects

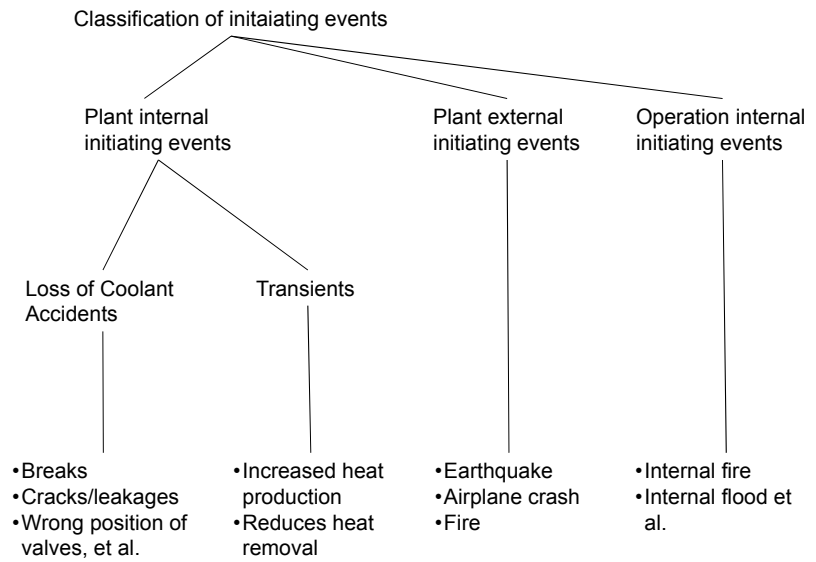
Initiating Events

Definition:

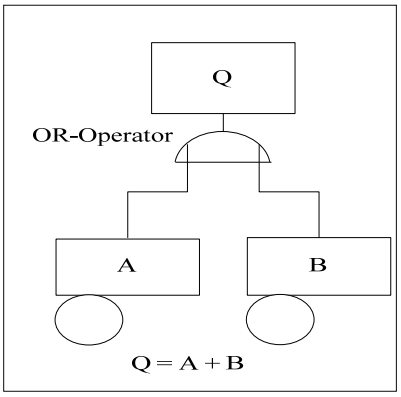
An initiating event is an incident which necessitates automatic or operator actions in order to bring the plant into safe steady state conditions; without such actions damage of the core may occur.

The tasks within a PRA level 1 are:

1. identification of the initiating events,
2. their classification into categories,
3. estimation of their frequencies.



Fault Tree Analysis I



Probability:

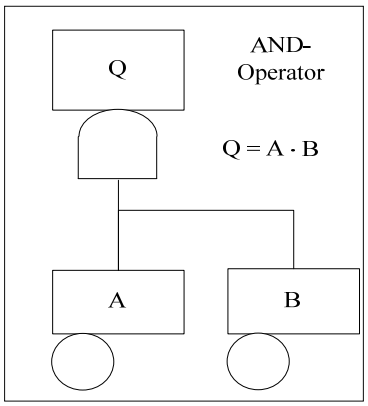
$P(Q) = P(A) + P(B) - P(A \cap B)$

$P(A) + P(B) - P(A) \cdot P(B|A)$

some conclusions:

1) A and B mutually exclusive:
   $P(A \cap B) = 0$
   $P(Q)=P(A) +P(B)$
2) A and B independent: $P(B|A) = P(B)$
   $P(Q)=P(A) +P(B) - P(A) \cdot P(B)$
3) A and B completely dependent: $P(B|A) = 1$
   $P(Q)=P(A) +P(B) - P(A)=P(B)$
   $P(Q)\approx P(A) +P(B)$
   always a conservative approach

Fault Tree Analysis II



Probability:

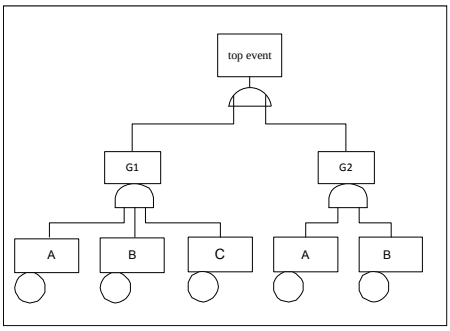
$P(Q) = P(A \cap B)$

$= P(A) \cdot P(B|A) = P(B) \cdot P(A|B)$

some conclusions:

1. A and B independent: $P(B|A) = P(B)$ and $P(A|B) = P(A)$:
   $P(Q) = P(A) \cdot P(B)$
2. A and B dependent:
   $P(Q) > P(A) \cdot P(B)$
3. total dependence: $P(B|A) = 1$
   $P(Q) = P(A)$
   approximations can be dangerous!

Fault Tree Analysis III



The systems fails (top event occurs), if cut sets

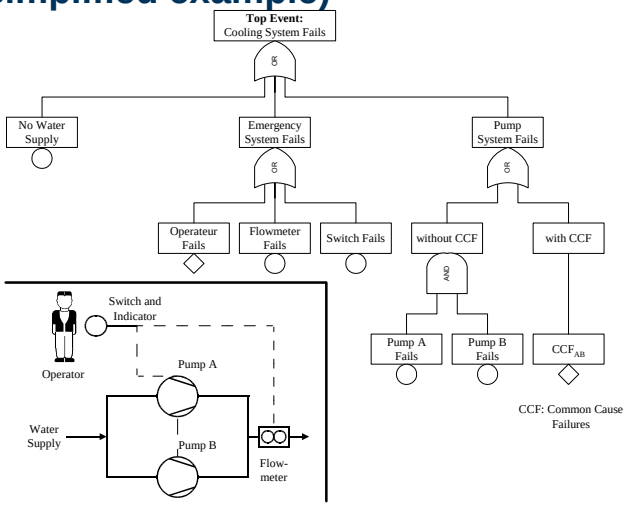
1. $A \cap B$
2. $A \cap B \cap C$

or minimal cut sets:

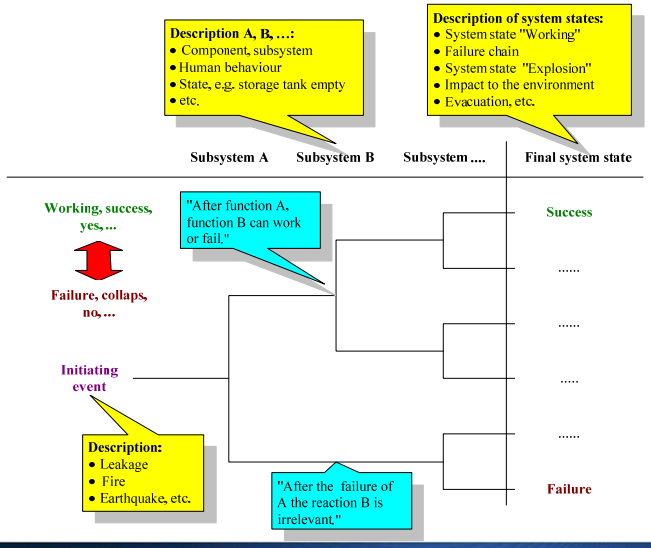
1. $A \cap B$

fail.

Flow Chart and its Fault Tree Representation (simplified example)

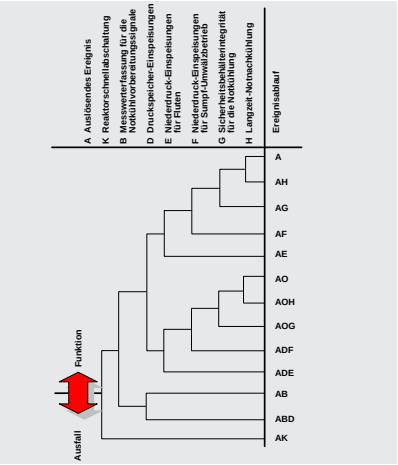


Construction of an event tree



Application of an Event Tree in Nuclear Energy

"Large leakage in the primary loop" of a NPP



Complete function

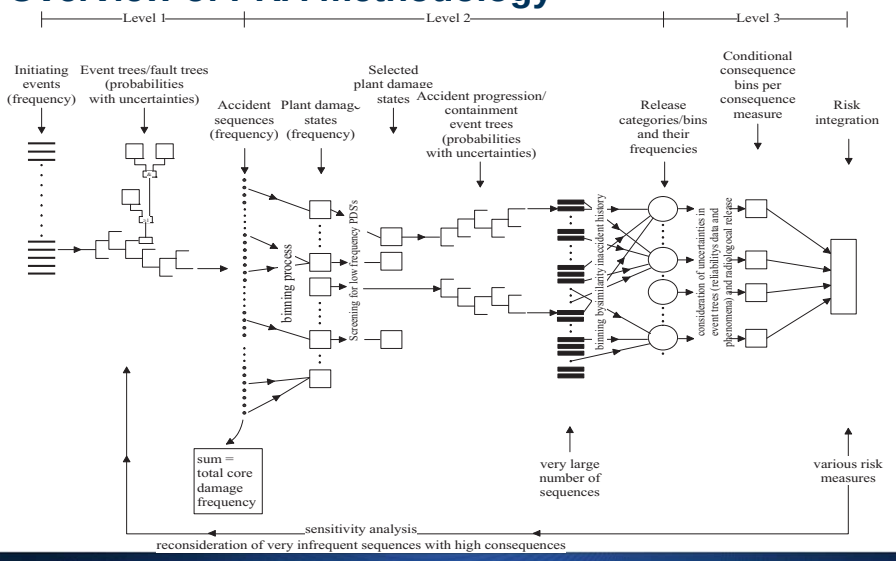
$Pr = Pr_A \cdot (1-q_K) \cdot (1-q_B) \cdot (1-q_D) \cdot (1-q_E) \cdot (1-q_F) \cdot (1-q_G) \cdot (1-q_H)$

q_i: dependent failure probability of a subsystem
Pr_A: probability of occurrence of the initiation event
Pr: probability of the complete path

Divergences between event tree and fault tree analysis

Fault tree	Event tree
Deductive	Inductive
Indicates the logic connection between events	Indicates the dependency of events which are set side by side (conditional probabilities)
A single chain of events from the “top event” to the basic event has no obvious importance (only sub fault trees)	All events along the chain from the initiating event to the final system state are of importance to the system
The system state at the knots aren’t indicated. The “top event” isn’t defining the system state (mostly the system failure)	Indicates many possible combinations of system/unit states and external events. The final state of a chain must be defined by the analyst.
	Better understanding of the role of human and external influences to the different system states
Statical approach	Dynamic processes are taken into account

Overview of PRA methodology



Characterization of a full PRA

Example: KKL, KKM

- Up to 100 initiating events (power operation + shut down states)
- Millions of accident sequences added to a total core damage frequency (CDF); combined use of fault tree and event tree techniques
- 8‘000 sequences (≥10-10 a^{-1}) binned into 20 plant damage states (PDS)
- 15 to 20 release categories and 10 to 15 damage indicators per release category formed